Cigital, Inc. (formerly Reliable Software Technologies)

Testing Security in E-Commerce

In 1997, computers were being networked on a global scale, which offered a limitless exchange of information, but also brought the risk of extensive damage from malicious programs. Businesses foresaw potential profits in electronic commerce, but worried whether the transfer of information, especially financial information, would be secure. Reliable Software Technologies (RST), a software research and development firm, had spent several years investigating methods to diagnose software vulnerabilities. In 1997, the company applied to the Advanced Technology Program (ATP) under the "Component-Based Software" focused program. The company proposed to develop a certification "pipeline," a gamut of tests through which a software component would progress. Once it passed the tests, a component would be given a digital stamp of approval. RST was concerned that as a small company, it did not have the resources to pursue the technology quickly enough to take advantage of a narrow window of opportunity. The company received a three-year cost-shared award for a project beginning in January 1998.

RST needed to establish a testing process that applied to individual components, but was also scalable to systems. The process would need validation in a commercial setting to prove its feasibility. However, by 1999, RST had concluded that component testing would not be marketable and instead concentrated on system-wide solutions. The company also shifted focus away from black-box testing techniques, in which the output of a program is analyzed but not the program itself, to the source code. It subsequently produced SourceScope to scan source code for vulnerability, issue a report, and suggest solutions. In 2003, RST, which had changed its name to Cigital, licensed SourceScope to Fortify Software. RST also uses SourceScope in consulting work with its own clients. Since its decision to bring SourceScope to market, the company has attracted $5 million in venture capital.

Throughout the project, the research team published articles and made presentations on security. Deloitte and Touche and the Virginia Chamber of Commerce named Cigital one of 50 fastest growing companies in Virginia. Inc. magazine twice included Cigital among the 500 top-performing firms. The company received widespread media coverage for discovering flaws in a gambling website and for confirming flaws in Java and Netscape Navigator.

COMPOSITE PERFORMANCE SCORE
(based on a four star rating)
* * * *

Research and data for Status Report 97-06-0005 were collected during January 2006.

Security Risks Threaten E-Business

In 1997, businesses were turning to the Internet to sell goods and services, but concerns about the security of private information were hindering consumers' adoption of electronic commerce. Encryption protected the data transmission medium but left server software and applications that were accessible over the Internet vulnerable to hackers, who could attack at either end of a transaction. Typically, software developers did not incorporate security mechanisms, which left Internet users at the mercy of ad hoc penetrate-and-patch methods that were usually applied only after a security breach had occurred. E-commerce represented a

potential market of more than $100 billion in 1997, according to analysts, making software security a high priority for businesses and the computer industry.

"There were no tools available to automatically scan for security holes in code," said Jeffery Payne, CEO of Reliable Software Technologies (RST), a software research and development firm. RST had been devising methods for testing software since its founding in 1992. The company had previously received an ATP award to develop its "Squeeze Play" technology to test and rate the reliability of software. The firm applied to ATP for an award under the "Component-Based Software" focused program in 1997. RST proposed to develop a rigorous process and core testing technologies for assuring the security of software components for e-commerce applications. While the proposed technology would be applicable to a wide range of software applications, the project would focus on Java components, which were broadly accepted by developers of software for the Internet. The company wanted to pursue this technology, but its limited assets would not allow it to proceed quickly enough to take advantage of a narrow window of opportunity.

E-commerce represented a potential market of more than $100 billion in 1997 making software security a high priority.

The company proposed a "security certification pipeline" that would integrate testing tools and processes to determine whether a failure in one component would corrupt other components. Once tested, if a component met minimum thresholds, RST's software would issue a digital "stamp of approval." The company also proposed to build a prototype environment for testing complete systems.

Among the technical challenges it faced, RST needed to establish testing processes that were rigorous enough to guarantee the security of software components for e-commerce. Processes would have to apply to individual components and also be scalable to systems. The company would develop the processes in-house and would then test them in a commercial setting. For this step, the company proposed to work directly with potential customers, who included software developers, vendors, integrators, and consultants.

Both the technology and the development process were radical departures from the industry norm and were virtually unheard of in 1997. Software companies put major emphasis on time-to-market, budgeting resources for fixing software in the next release.

The company applied for and received an ATP cost-shared award for a three-year project that began in January 1998.

RST Investigates Security Testing

RST classified the security threats into three categories:

1) Mobile code, or software obtained from remote systems, transferred across a network, and downloaded and executed on a local system without explicit installation or execution by the recipient (for example, JavaScript, VBScript, Java applets, ActiveX controls, and macros embedded in Microsoft Office documents)
2) Security holes in e-commerce systems
3) Smart card application software

If successful, the security certification pipeline would be used to analyze all three categories.

The company began the ATP-funded project by identifying technologies to certify the secure behavior of software components. The project researchers reused some of the source code analysis algorithms developed during its previous ATP-funded project for "white-box" testing techniques, which are used when a component's programming code is known. To assess the security of components for which the source code is not available, the project also examined "black box" techniques, which check that a program performs as expected. Black box testing examines the output of a program rather than the program itself. Based on the methodology the researchers developed, they began building a test bench, which is a virtual testing environment that enables mimicking a running system, for certifying software components for security.

The company pursued relationships with companies to validate and test its software. In August 1998, RST announced that it had been hired by Visa to test its prototype smart card, a credit card with an embedded microprocessor that stores information and monetary value and serves as a form of identification in electronic systems. Using early technical results of the project as a starting point, RST developed an automated security-testing suite that analyzed and identified security vulnerabilities in the cards. The company used the suite primarily in its consulting work for customers, but also licensed it to MasterCard and the National Security Agency as well as Visa.

Key RST personnel made presentations at conferences on Internet security and published articles in journals on the developing methodology for security testing. They continued to share their research throughout the duration of the project.

By the second year of the project, RST reported that the ATP-funded project was becoming increasingly central in its planning as the company made software certification its primary mission. The company developed a prototype system to scan for buffer overflow, which occurs when a process attempts to store more data in a buffer than there is memory allocated for it. This situation can cause a process to crash or produce incorrect results. After such an overflow has occurred, a system will be in a state that developers did not plan for, and it may be vulnerable to attack. Such overflows can be triggered by malicious code and were a major vulnerability in the most common code, which was written in the C programming language.

In January 1999, the RIA Group hired RST to test its web-based search and retrieval systems. RIA provided specialized tax and business information and released a new version of its software every 45 days.

Company Grows Quickly and Gains Recognition

In 1999, the Virginia Chamber of Commerce named RST a “Fantastic 50” winner and recognized it as the fourth fastest growing Virginia technology company. In addition, Deloitte and Touche named it a “Technology Fast 50” winner. The company moved to a new building and doubled its space. By this time, demand for application server software had altered the project’s scope. RST determined that security vulnerabilities with Java were tied to specific Java implementations rather than the Java language itself; as a result, RST chose to focus on C code.

In September of that year, CNN, Headline News, and *The New York Times* ran stories on RST’s success in discovering a flaw in an Internet gambling site's software that would allow users to bilk other players. A few months later, RST gained similar exposure when it discovered a security flaw in Netscape Navigator. By October, RST had twice discovered or confirmed a serious security flaw in versions of the Java Virtual Machine. “The flaw allows an attacker to create a booby-trapped Web page, so that when a victim views the page, the attacker seizes control of the victim’s machine and can do whatever he wants,” according to RST’s analysis.

The company attracted customers in software, financial services, and related industries. The Federal Reserve Bank of New York hired RST to test its e-commerce systems, implement a mobile code security policy, and improve overall electronic security. In 2000, RST changed its name to Cigital, Inc. as it moved to a consulting business model whereby it worked with companies throughout the life cycle of software installations.

RST needed to establish testing processes that were rigorous enough to guarantee the security of software components for e-commerce.

In the third year of the ATP-funded project, Cigital investigated how its security certification methodology worked on systems built from JavaBeans, which are reusable software components written in the Java programming language. Cigital developed thresholds that components must meet to be certified and ways to test the security of the components’ behavior when combined. When the company found no significant market for tools to look at security component-by-component, it redirected the project. The researchers realized that the key technology from the project was the source code scanner. The scanner could look at overall system security through a single scanning system for known vulnerabilities and then monitor the

code during execution, looking for a very limited number of specific system actions. RST deferred work on creating a digital signature that identified a successfully tested component, which did not appear to have commercial promise.

Work Continues on Scanner

After ATP funding ended in 2001, Cigital continued to focus on the scanner. No other source code scanners existed, which made it difficult for the company to interest venture capitalists, who felt that security was a network problem, not an application problem. Cigital instead actively pursued strategic partnerships with risk management consulting firms, insurance companies, and solution providers. It simplified the scanner developed during the ATP-funded project and soon made it available as a public domain tool called ITS4.

"We wanted to put something out into the public domain that would attract interest to code scanning without putting all of our intellectual property in it," said Payne. “We hoped that a free version of a code scanner would drive a need for commercially available tools that were supported and maintained.” When 10,000 users downloaded ITS4, the company recognized the extent of interest in source code scanning and pursued a commercial model.

Using feedback from the users of ITS4, the company incorporated the algorithms developed during the ATP-funded project into a more complex security code scanner, SourceScope, which scanned source code, issued a report, and suggested solutions for vulnerabilities. Two commercial developments emerged from this initiative. First, one of the key people on the ATP project had left Cigital in early 2001 to start Secure Software, a competitor that sells a code analysis tool inspired by the technology from the ATP-funded project. Second, in 2003, Cigital licensed SourceScope to a start-up company, Fortify Software. This product, renamed the Fortify Software Code Analysis Tool, is now Fortify’s flagship product. Cigital has a strategic relationship with Fortify Software, receives quarterly royalties, owns one percent of the company, and provides consulting services related to the tool.

Payne said he sees growing awareness of the need for Cigital’s security services. “The true cost of security breaches is not the direct cost to correct the issue, but the damages to the brand and market demand that occur. One of our customers had a software breach that caused their market value to drop $500 million when it was disclosed to the press. Many of our customers are concerned about the tens if not hundreds of millions of dollars they will lose in value if their customer data or credit card information is compromised.”

When 10,000 users downloaded ITS4, the company recognized the extent of interest in source code scanning and pursued a commercial model.

He added that without ATP’s support, the project would never have happened because of the initial lack of investor interest in the technology. ATP filled the need for bridge financing between an idea and a prototype. Since beginning work on the commercial version of the scanner, the company has attracted $5 million in venture capital.

Conclusion

Since the early 1990s, businesses have been interested in the Internet as a new and profitable route for selling goods and services. The main drawback to online commerce was the apparent vulnerability of software applications to hackers. In 1997, Reliable Software Technologies, Inc. (RST) applied to ATP under the "Component-Based Software" focused program. The company had developed methods for testing software's reliability with the help of a previous ATP award (“A Plausible Dependability Model for Component-Based Software,” # 95-09-0021). In this second ATP-funded project, which began in 1998, RST proposed a series of tests that would expose potential flaws in web-based software and would certify software that passed the test with a digital "stamp of approval."

The project achieved its goals of building core testing technology for software security. The rigorous tools that emerged, however, did not find a significant market because customers were not interested in component-by-component testing. The company refocused on a program to scan source code. Toward the end of the project, the company changed its name to Cigital.

Shortly after the project ended, Cigital simplified the prototype it had developed and then released ITS4, a public domain tool to test software vulnerability and prescribe solutions to the revealed flaws. When 10,000 users downloaded the program, the company knew that a code-scanning tool had commercial possibility. It developed a more complex version of this tool, SourceScope, which it licensed in 2003 to Fortify Software. The licensee has made the tool its flagship product, while Cigital uses SourceScope with its own clients. In addition, the company attracted $5 million in venture capital to bring the scanner to market.

The project research was the source of numerous articles by the staff, as well as presentations at conferences on security, including one convened and sponsored by Cigital. The company revealed flaws in Netscape Navigator and Java platforms. Furthermore, it revealed how gambling websites could be used to cheat participants, revelations that received major news media coverage and demonstrated the value of the technology to a wide audience.

PROJECT HIGHLIGHTS
Cigital, Inc. (formerly Reliable Software Technologies)

Project Title: Testing Security in E-Commerce (Certifying Security in Electronic Commerce Components)

Project: To design a rigorous process and core testing technologies for assuring the security of software components, a key enabling technology for Internet-based electronic commerce.

Duration: 1/2/1998 - 1/1/2001
ATP Number: 97-06-0005

Funding (in thousands):

ATP Final Cost	$1,978	83.9%
Participant Final Cost	380	16.1%
Total	$2,358	

Accomplishments: With ATP funding, Reliable Software Technologies (RST), which was renamed Cigital in 2000, accomplished the following:

- Developed a rigorous process and tools to diagnose vulnerabilities in web-based software applications
- Wrote a program that scans source code for vulnerabilities, issues a report, and suggests solutions
- Received widespread media coverage for discovering flaws in a gambling website and for confirming flaws in Java and Netscape Navigator
- Was named by Deloitte and Touche and the Virginia Chamber of Commerce as one of the 50 fastest growing companies in Virginia and was twice named by Inc. magazine among the 500 top-performing firms

Commercialization Status: The ATP-funded technology was the basis for two products. One was developed by a former RST colleague who is now a competitor. Cigital uses the second product, SourceScope, in its work with its own clients and also licenses it to Fortify Software, in which it owns a percentage and with which it maintains a consulting relationship.

Outlook: The outlook for this technology is strong. Because security is a critical concern with online transactions, the market for tools to spot flaws and prevent their exploitation is robust.

Composite Performance Score: * * * *

Number of Employees: 35 at start of project; 100 as of January 2006

Focused Program: Component-Based Software, 1997

Company:
Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166

Contact: Jeffery Payne
Phone: (703) 404-9293

Publications:

- Ghosh, A.K. “Securing E-commerce: A Systematic Approach.” *Journal of Electronic Commerce*, 2, September 1997.
- Ghosh, Anup K. *E-Commerce Security: Weak Links, Best Defenses.* New York: John Wiley and Sons, 1998.
- Ghosh, A.K. "E-commerce Security: No Silver Bullet." *Database Security XII: Status and Prospects*. IFIP International Federation for Information Processing , Vol. 14 Heidelberg: Springer Verlag, 1999.
- McGraw, Gary and Ed Felten. *Securing Java: Getting Down to Business with Mobile Code*. New York: John Wiley and Sons, 1999.
- Voas, Jeffrey. “Developing a Usage-Based Software Certification Process.” *IEEE Computer Society* 33, pp. 27-32 August 2000.
- Walls, T.J., V. Shah, and A.K. Ghosh. “Towards Certifying Software for Security.” International Security Assurance Certification Conference (ISACC) 2000, September 2000.

Presentations:

- Ghosh, A.K. “Certifying Security of Components Used in Electronic Commerce.” Workshop on Compositional Software Architectures, Monterey, CA, January 6-9, 1998.
- Ghosh, A.K. “E-Commerce Security: Protecting Your Clients, Your Reputation, and Your Profit.” NetExpo Washington, Washington, D.C., September 9, 1998.

PROJECT HIGHLIGHTS
Cigital, Inc. (formerly Reliable Software Technologies)

- Ghosh, A.K. “Security in Internet Electronic Commerce,” Defending Cyberspace, Washington, D.C., September 24, 1998.

- Ghosh, A.K., and Gary McGraw. “An Approach for Certifying Security in Software Components.” Crystal City, VA, October 6-9, 1998.

- Ghosh, A.K. “On Certifying Mobile Code for Secure Applications.” International Symposium on Software Reliability Engineering, Paderborn, Germany, November 4-7, 1998.

- Ghosh, A.K. “Certifying Electronic Commerce Software for Security.” Workshop on Electronic Commerce and Web Information Systems, Santa Clara, CA, April 9-10, 1999.

- Ghosh, A.K. “Securing the Future of E-Commerce.” E-Gov99, the National Electronic Government Conference and Exposition, Washington, D.C., June 28-July 1, 1999.

- Leslie, R.A., and V. Shah. “Demonstration of Security Analysis of C Programs.” ATP National Technology Showcase Exhibit, San Jose, CA, November 1999.

- Ghosh, A.K. “Securing E-Commerce Transactions.” Make the Most of E-Commerce, Maryland High Technology Council Conference, Bethesda, MD, March 14, 2000.

- Ghosh, A.K. Keynote Address, Conference on E-Commerce Applications, Quality Assurance Institute, Kansas City, MO, June 14, 2000.